Context

Data Classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled / secured and is also indicative of its value in terms of Business Assets.

This document presents a data classification system which groups information into four hierarchical levels: from level 1 that covers the least sensitive type of information through level 4 which is aimed at the most important data and processes. The hierarchical nature of this systems means that each level is a superset of the previous level. For example, if a system is classified as level 2, then the system must follow the directives of levels 1 and 2. If a document or system contains data that falls into more than one sensitivity level, it must be classified according to the needs of the most confidential data on the document or system.

This classification covers the electronic equivalent of documents for the most part, although it should be easy to devise appropriate measures for any physical document.

Classification of information

Level 1: Public Information

Description: Data of this type could be made public without any implications for the company (i.e. the data is not confidential). Data integrity is not vital. Loss of service due to malicious attacks is an acceptable danger. Examples: Test services without confidential data, certain public information services.

Guidelines on storage: none

Guidelines on transmission: none

Guidelines on destruction: none

Level 2: Internal Information

Description: External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g. at worse, the company may be publicly embarrassed). Internal access must be somewhat restricted. Data integrity is important

but not vital. Examples of this type of data are found in development groups (where no live data is present), certain production public services, certain Customer Data, "normal" working documents and project/meeting protocols as well as internal telephone books.

Guidelines on storage:

1. Information shall be labeled. i.e. the classification level should be written on documents, media (tapes, diskettes, disks, CD's etc), electronic messages and files.
2. IT Systems susceptible to virus attacks should be regularly scanned for viruses. The integrity of systems should be regularly monitored.

Guidelines on transmission:

1. For projects involving collaboration with external partners, a project policy document shall stipulate what information may be shared with the external partners.
2. This information shall stay within the company, if it must transit through public media (e.g. the Internet), it should be encrypted.
3. Apart from the exceptions defined above, internal data shall not be transferred outside the company.

Guidelines on destruction: none

Level 3: Confidential Information

Description: Data in this class is confidential within the company and protected from external access. If such data were to be accessed by unauthorized parties, it could influence the company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause a major drop in customer confidence. Data integrity is vital. Examples: salaries, personnel data, accounting data, very confidential customer data, sensitive projects and confidential contracts. Data centers normally maintain this level of security.

Guidelines on storage:

1. Information shall be labeled. i.e. the classification level should be written on documents, media (tapes, diskettes, disks, CD's etc), electronic messages and files.

2. IT systems susceptible to virus attacks should be regularly scanned for viruses. The integrity of systems should be regularly monitored. IT systems shall be configured to protect against unauthorized modification of data and programs.
3. Information shall be kept under lock and key (e.g. documents in locked cabinets, computers in locked rooms).

Guidelines on transmission:

1. Shared secrets (passwords) should not be transmitted in clear-text (electronically or on paper).
2. This information shall stay within the company, if it must transit through public media (e.g. the Internet), it must be encrypted. Encryption algorithms used should be strong.[1]

Guidelines on destruction:

1. Information shall be securely disposed of when no longer needed (e.g. shredding of documents, destruction of old disks and diskettes as well as any backup media, etc.).

Level 4: Secret Information

Description: Unauthorized external or internal access to this data is detrimental to the company. Data integrity is vital. Access to this data must be limited to a very small number of people and must be controlled with very strict rules. Examples: information about major pending contracts/reorganization/financial transactions or application architecture data.

Guidelines on storage:

1. Information shall be labeled. i.e. the classification level should be written on documents, media (tapes, diskettes, disks, CD's etc), electronic messages and files.
2. IT systems susceptible to virus attacks shall be regularly scanned for viruses. The integrity of systems shall be regularly monitored. IT systems shall be configured

[1] RCA 1024-bit, IDEA, 3DES etc. not simple mechanisms like XOR. Note that normal DES is no longer considered strong.

to protect against unauthorized modification of data / programs and shall be audited regularly (yearly at a minimum).

3. Information shall be kept under lock and key (e.g. documents in locked cabinets, computers in locked rooms).
4. Information shall be stored in encrypted format or on removable media which are physically secured.

Guidelines on transmission:

This information shall be encrypted during transmission outside of secure zones. Encryption algorithms used shall be strong.[2]

Guidelines on destruction:

Information shall be securely disposed of when no longer needed (e.g. shredding of documents, destruction of old disks and diskettes etc.). Document footprints on media must be deleted using a strong algorithm.

Prescriptions

- All data has an owner.
- The data or process owner must classify the information into one of the security levels- depending on legal obligations, costs, corporate into policy and business needs.
- If the owner is not sure at what level data should be classified, use level 3, Confidential.
- The owner must declare who is allowed access to the data.
- The owner is responsible for this data and must secure it or have it secured (e.g. via a security administrator) according to it's classification.
- Once the data on a system has been classified to one of the following levels, then that system should be installed to conform to all directives for that class and classes below. Each level is a superset of the previous level. For example, if a system is classified as level 3 , then the system must follow the directives of level 1,2 and 3 .

[2] RCA 1024-bit, IDEA, 3DES etc. not simple mechanisms like XOR. Note that normal DES is no longer considered strong.